An overview of [Organisation Name]'s approach to information security based upon the ISO 27001:2022 standard.

INFORMATION SECURITY MANUAL

Classification: Internal

This document may only be shared internally without prior confirmation from the owner. Anyone sharing it externally should first seek the owner's written permission.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Introduction to the ISO 27001 Handbook

Purpose of the Handbook

This handbook comprehensively overviews how [Organisation Name] meets the ISO/IEC 27001:2022 standard requirements.

Commented [AP1]: Search and replace [Organisation Name] throughout the document to replace the company name.

The document serves as a guide to demonstrate compliance with each clause of the standard, facilitating a clear understanding of our Information Security Management System (ISMS) for internal stakeholders and external auditors.

Intended Audience

This handbook is intended for the following audiences:

- **Internal Stakeholders** - Management, information security teams, and all employees are included to ensure awareness and understanding of their roles and responsibilities in maintaining the ISMS.
- **External Auditors** - To provide a quick reference tool that points to the relevant policies, procedures, and records, streamlining the audit process and demonstrating our compliance with the ISO/IEC 27001:2022 standard.
- **Partners and Clients** - To offer transparency into our information security practices, reinforcing their confidence in our commitment to protecting information assets.

Key Comments and Observations

(This section is for the person adjusting the template to note any specific comments or observations relevant to the application of this handbook.)

Scope of the ISMS

The Organisational Context (Clause 4.1)

[Organisation Name] has evaluated external and internal issues relevant to its purpose, affecting its ability to achieve the intended outcomes of its Information Security Management System (ISMS).

These issues are documented in the ISMS scope document.

Supporting Materials	Description
Information Security Management System (ISMS) Scope Document	The 'Context of the Organisation' section outlines the internal and external issues impacting the organisation's ISMS.

Commented [AP2]: It is quite alright to remove these sections, which currently point at parts of other documents, and summarise the contents directly. i.e. put in a scope statement, and say 'for further information see….'

The Needs and Expectations of Interested Parties (Clause 4.2)

[Organisation Name] has identified and documented the needs and expectations of interested parties relevant to the ISMS.

Supporting Materials	Description
Information Security Management System (ISMS) Scope Document	Stakeholders are outlined in the ISMS scope document under the 'Interested Internal Stakeholders' and 'External Stakeholders' sections.

The Scope of the ISMS (Clause 4.3)

[Organisation Name] has evaluated the boundaries and applicability of the ISMS to determine its scope, considering and documenting the external and internal issues and the needs and expectations of interested parties.

Supporting Materials	Description
Information Security Management System (ISMS) Scope Document	The boundaries are outlined in the sections' Physical & Logical Boundaries' and 'Organisational Boundaries'.

Information Security Leadership

Leadership and Commitment (Clause 5.1)

Senior management at [Organisation Name] demonstrates leadership and commitment to the ISMS by ensuring the information security policy and objectives are established and aligned with the organisation's strategic direction.

The leadership ensure integration of the ISMS requirements into business processes, allocates necessary resources, communicates the importance of effective information security, ensures the ISMS achieves intended outcomes and promotes continual improvement.

Supporting Materials	Description
Information Security Statement	The information security statement is an example of commitment to data security within our organisation and is shared with all staff.
Information Security Group: Terms of Reference	The Information Security Group (ISG) has senior staff members in attendance. The group provides strategic direction, prioritisation of efforts, necessary resources and senior review.

Information Security Policy (Clause 5.2)

[Organisation Name] has established a collection of information security policies appropriate to its purpose.

The main Information Security Policy includes directions on security objectives, commitments to meet applicable requirements, and continual improvement of the ISMS. It also directs readers to the supporting policies outlined below.

The policy is documented, communicated within the organisation, and available to interested parties.

Supporting Materials	Description
Information Security Policy	The overarching parent policy summarises general conditions across the organisation for all stakeholders.
Acceptable Use Policy	Defines acceptable and unacceptable use of the organisation's information systems and resources.
Access Control Policy	Specifies the requirements for

	controlling access to information and information systems.
BYOD Policy	Establishes rules and guidelines for using personal devices to access company data and systems.
Data Protection Policy	Details measures and practices to protect personal data in compliance with relevant regulations.
Data Retention Policy	Sets out the principles for retaining and disposing of data securely and competently.
Mobile Device Policy	Provides guidelines for the secure use of mobile devices within the organisation.
Password Policy	Defines the requirements for creating, managing, and protecting passwords.
Patching Policy	Describes the process for managing software patches and updates to maintain security.
Secure Development Policy	Outlines best practices for developing and maintaining secure software applications.
Supplier Security Policy	Establishes security requirements for engaging and managing third-party suppliers.
Asset Management Policy	Details procedures for managing information assets throughout their lifecycle.
Cloud Services Policy	Provides guidelines for the secure use and management of cloud services.
Remote Working Policy	Specifies security measures and practices for employees working remotely.

Organisational Roles, Responsibilities, and Authorities (Clause 5.3)

Top management at [Organisation Name] ensures that responsibilities and authorities for roles relevant to information security are assigned and communicated. They are responsible for ensuring that the ISMS conforms to ISO/IEC 27001 requirements and reporting on ISMS performance to top management.

Supporting Materials	Description

ISMS Roles & Responsibilities Document	A summary of the key ISMS responsibilities by role.

Planning & Risk Management

Actions to Address Risks and Opportunities (Clause 6.1)

[Organisation Name] has identified and documented the risks and opportunities that must be addressed to ensure the ISMS can achieve its intended outcomes, prevent undesired effects, and achieve continual improvement.

These actions include planning to address risks and opportunities and integrating them into the ISMS processes.

General

[Organisation Name] considers the issues impacting the organisation, referred to in Clause 4.1 and the requirements of interested parties in Clause 4.2. It determines the risks and opportunities that must be addressed to ensure the ISMS achieves its intended outcomes, prevents or reduces undesired effects, and achieves continual improvement.

Supporting Materials	Description
Risk Assessment & Treatment Methodology	Outlines the overall approach to risk, including risk identification, assessment, prioritisation, mitigation, monitoring, treatment plans and escalations paths.

Information Security Risk Assessment (Clause 6.1.2)

[Organisation Name] has defined and applied an information security risk assessment process.

The process includes establishing and maintaining information security risk criteria, ensuring repeated risk assessments produce consistent, valid, and comparable results, identifying information security risks, analysing these risks, and evaluating them against established risk criteria.

Supporting Materials	Description
Risk Assessment & Treatment Methodology	Outlines the approach and scoring criteria for risk assessments.
Risk Log	Records of each risk and its assessment.

Information Security Risk Treatment (Clause 6.1.3)

[Organisation Name] has defined and applied a process for treating information security risks. This includes selecting appropriate risk treatment options, implementing risk treatment plans, and retaining documented information about the information security risk treatment process.

A Statement of Applicability outlining the controls laid out by ISO 27001:Annex A is also maintained.

Supporting Materials	Description
Risk Assessment & Treatment Methodology	Outlines the approach and scoring criteria for risk assessments.
Risk Treatment Plans	Risk Treatment Plans (RTPs) exist for all significant risks.
Statement of Applicability	A summary of 93 controls and their applicability to the organisation and its scope.

Information Security Objectives (Clause 6.2)

[Organisation Name] has established information security objectives, which have been approved by senior management.

The objectives are consistent with the information security policy, measurable (if practicable), take into account applicable information security requirements, are monitored, communicated, updated as appropriate, and are available as documented information.

Supporting Materials	Description
ISMS Objectives	Approved objectives for the ISMS for the current period.

Handling Changes to the ISMS

When [Organisation Name] determines the need for changes to the ISMS, these changes are carried out in a planned manner. This includes considering the changes' purpose and potential consequences, the integrity of the ISMS, the availability of resources, and the allocation or reallocation of responsibilities and authorities.

A change management policy is in place, providing flexibility to allow the system to be used for any proposed change to the ISMS. Changes will be evaluated, implemented and communicated to appropriate stakeholders.

Any technology changes will be managed via the IT Change Management Process and evaluated for potential negative impacts on confidentiality, integrity and availability.

Supporting Materials	Description
ISMS Change Management Policy	A policy which outlines the expectations around changes to the ISMS and how they should be processed.
ISMS Change Request Records	Record any requests for changes to the ISMS, along with Minutes of ISG meetings.
IT Change Management Process	A process for the request, management and approval of changes to IT services.
Requests for Change (RFCs)	Records of technical changes and approval.
Communication Records	Including emails, release notes, meeting notes, and other communications aligned with any changes.

Supporting the ISMS

Resources (Clause 7.1)

[Organisation Name] has determined and provided the resources to establish, implement, maintain, and continually improve the ISMS.

Supporting Materials	Description
Resource Allocation Plan	This document summarises the human, technical, training & financial resources needed for the ISMS for the forthcoming period.

Competences of Staff (Clause 7.2)

[Organisation Name] has determined the necessary competence of persons doing work under its control, which affects its information security performance.

The organisation ensures that these persons are competent based on appropriate education, training, or experience and retains appropriate documented information as evidence of competence.

Supporting Materials	Description
Training & Competency Matrix	Outlining the key roles within the ISMS and the required and current competencies in a gap analysis, thereby identifying current training needs.
Records of Training	Records each individual's training activities and certifications within the Training & Competency Matrix.

Awareness Programme (Clause 7.3)

Persons working under [Organisation Name]'s control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the benefits of improved information security performance, and the implications of not conforming to the ISMS requirements. An ongoing awareness and communication plan evidences this.

Supporting Materials	Description
Information Security Policy (and supporting policies)	Outlines key responsibilities for staff. Policies are made available at the point of induction for new employees and

	thereafter regularly as they are refreshed. Policies are shared at their regular review points. Policies are also part of the ongoing communications & awareness plan.
ISMS Roles & Responsibilities Document	Outlines the key expectations for those directly involved in the ISMS.

Communication Plans (Clause 7.4)

[Organisation Name] has determined the need for internal and external communications relevant to the ISMS, including what to communicate, when to communicate, with whom to communicate, and how to communicate.

Supporting Materials	Description
Information Security Communications Plan	Provides details on the ISMS campaign for the forthcoming period.

Documented Information Handling (Clause 7.5)

[Organisation Name]'s ISMS includes documented information required by the ISO/IEC 27001 standard and documented information determined by the organisation as necessary for the effectiveness of the ISMS.

Creating and Updating (Clause 7.5.2)

When creating and updating documented information, [Organisation Name] ensures appropriate identification, description, format, and media and reviews and approves suitability and adequacy through a document control procedure and register of ISMS documentation.

Supporting Materials	Description
Control of Documents Within The ISMS	Instructions on how to manage documentation for the ISMS
ISMS Document Register	A list of all key ISMS documents

Control of Documented Information (Clause 7.5.3)

Documented information required by the ISMS and by ISO/IEC 27001 is controlled to

ensure it is available, suitable for use, where and when needed, and adequately protected. Guidance is provided regarding the control, update, and disposal of documents.

Supporting Materials	Description
Document Control Register	A list of all key ISMS documents

Operation of the ISMS

Operational Planning and Control (Clause 8.1)

[Organisation Name] has planned, implemented, and controls the processes needed to meet the ISMS requirements and to implement the actions determined in Clause 6.

This includes establishing criteria for the processes, implementing control of the processes per the criteria, and maintaining documented information to have confidence that the processes have been carried out as planned.

Supporting Materials	Description
A variety of documented operational procedures	All key information security processes are documented, and staff are trained in their application. Each process should maintain a record of tracking changes (e.g. adding users to the system), including who, what and when.
ISMS Change Management Policy	A policy which outlines the expectations around changes to the ISMS and how they should be processed.
ISMS Change Request Records	Record any requests for changes to the ISMS, along with Minutes of ISG meetings.
IT Change Management Process	A process for the request, management and approval of changes to IT services.
Requests for Change (RFCs)	Records of technical changes and approval.

Information Security Risk Assessment (Clause 8.2)

[Organisation Name] performs information security risk assessments at planned intervals and when significant changes are proposed or occur. This ensures that information security risks are identified, analysed, and evaluated.

A risk assessment and treatment methodology are outlined in section 6.2. Risks will be assessed and recorded in the Risk Log and any Request for Change (RFC) documents.

Supporting Materials	Description
Risk Log	Records of each ISMS risk and its assessment.
Request for Change (RFC)	Records of change to infrastructure and services

Information Security Risk Treatment (Clause 8.3)

[Organisation Name] applies a systematic approach to information security risk treatment. This involves selecting appropriate risk treatment options, implementing risk treatment plans, and retaining documented information about the information security risk treatment process.

The risk treatment methodology is outlined in section 6.2. Risk Treatment Plans (RTPs) will be maintained for all risks that meet the criteria.

Supporting Materials	Description
Risk Treatment Plans	Records of each ISMS risk and its treatment plan.
Request for Change (RFC)	Records changes and the risk treatments to infrastructure and services.

ISMS Performance Evaluation

Monitoring, Measurement, Analysis, and Evaluation of the ISMS (Clause 9.1)

[Organisation Name] determines what needs monitoring and measuring, including information security processes and controls.

The organisation ensures that the monitoring, measurement, analysis, and evaluation methods are valid and performs these activities at planned intervals to evaluate the ISMS's information security performance and effectiveness.

Supporting Materials	Description
Metrics & Reporting Approach	A summary of the key metrics, KPIS, methods and frequency of reporting across the ISMS
Monthly Information Security Metrics Report(s)	Monthly reports for senior management regarding the ISMS operation

Internal Auditing (Clause 9.2)

[Organisation Name] conducts internal audits at planned intervals to provide information on whether the ISMS conforms to the organisation's requirements and the ISO/IEC 27001 requirements and is effectively implemented and maintained.

Supporting Materials	Description
Internal Audit Procedure	Details of how audits are conducted and expected outputs
Internal Audit Findings Report(s)	Reports generated by the internal audits

Internal Audit Programme (Clause 9.2.2)

[Organisation Name] establishes an internal audit programme, including the frequency, methods, responsibilities, planning requirements, and reporting of its internal audits. This ensures that audits are conducted systematically, based on the importance of the processes concerned and the results of previous audits.

Supporting Materials	Description
Internal Audit Plan	Outlines the current programme of activities around internal auditing for the current period.

Management Reviews

Top management at [Organisation Name] reviews the organisation's ISMS at planned

intervals to ensure its continuing suitability, adequacy, and effectiveness.

Supporting Materials	Description
Information Security Steering Group Terms of Reference	Outlining the responsibilities of the group, frequency of review and activities.

Management Review Inputs (Clause 9.3.2)

The inputs to the management review include the status of actions from previous management reviews, changes in external and internal issues, information security performance, feedback from interested parties, risk assessment and risk treatment results, and opportunities for continual improvement.

Supporting Materials	Description
Internal Audit Findings Report(s)	Reports generated by the internal audits
Monthly Information Security Metrics Report(s)	Monthly reports for senior management regarding the ISMS operation

Management Review Results (Clause 9.3.3)

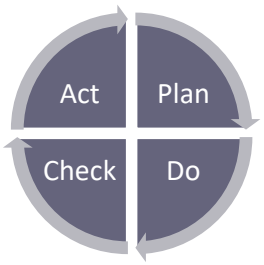
The results of the management review include decisions related to continual improvement opportunities and any need for changes to the ISMS.

Supporting Materials	Description
Information Security Group Meeting Minutes	Records of meeting minutes, including actions and decisions.

Continual Improvement

Continual Improvement (Clause 10.1)

[Organisation Name] continually improves the ISMS's suitability, adequacy, and effectiveness by enhancing its processes and controls based on monitoring, measurement, analysis, and evaluation results.



Our senior management plays an active role in setting annual objectives, reviewing and monitoring the ISMS's performance, and supporting progress with internal and external auditing to ensure that the ISMS continually seeks improvement.

Each process and objective must be supported with a continual improvement approach.

Continual improvement within [Organisation Name] is multi-faceted, involving the following;

- **Leadership and Commitment**: Senior management sets objectives, reviews performance, and allocates resources for ISMS improvement.
- **Systematic Monitoring and Review**: Regular internal and external audits to identify areas for improvement and ensure ISO/IEC 27001 compliance.
- **Risk Management**: Continuous risk assessments and implementation of appropriate controls to mitigate risks.
- **Training and Awareness**: Regular training programs to enhance staff information security awareness and competencies.
- **Feedback and Improvement**: Actively seek and address stakeholder feedback to identify improvement opportunities.
- **Technological Advancements**: Adapting to new challenges by staying abreast of technological advancements and emerging threats.
- **Documentation and Communication**: Documenting and effectively communicating all changes and improvements to the ISMS.

Nonconformities and Corrective Actions (Clause 10.2)

Nonconformities are outcomes where there are deviations from the ISO 27001 standard or the expected working of the ISMS.

When a nonconformity occurs, [Organisation Name] reacts to the nonconformity and,

as applicable:

1. Takes action to control and correct it.
2. Deals with the consequences.

[Organisation Name] evaluates the need for action to eliminate the causes of nonconformity to ensure it does not recur or occur elsewhere by:

1. Reviewing the nonconformity.
2. Determining the causes of the nonconformity.
3. Determining if similar nonconformities exist or could potentially occur.

Actions needed are implemented, the effectiveness of any corrective action taken is reviewed, and changes to the ISMS are made if necessary. Corrective actions are appropriate to the effects of the nonconformities encountered.

Supporting Materials	Description
Internal Audit Findings Report	The internal audit report(s) will act as a source of input where deviations are found with the ISO 27001 standard.
Corrective Actions Log	All corrective actions will be captured in a central log for review and allocation of ownership.